Securing Kubernetes Environments with StackRox

Degree programme : BSc in Computer Science
Thesis advisor : Lukas Ith
Expert : Dr. Joachim Wolfgang Kaltz
Industrial partner : Adfinis AG, Bern

Tracking vulnerabilities in containerized environments is challenging due to their complexity. StackRox is a tool designed to enhance security in Kubernetes environments by providing visibility and control over containerized applications. This thesis evaluates StackRox‘s effectiveness and integration into Adfinis‘s processes, addressing gaps and developing deployment scenarios to improve security management both internally and for customer environments.

Overview

Ensuring security in containerized environments is complex. At Adfinis, this responsibility has been manually managed, with technology owners needing to stay updated on vulnerabilities and notify relevant parties for patching. This approach lacks automation, making it difficult to keep up with evolving security threats. Prior to this thesis, StackRox, a security platform designed to enhance Kubernetes security by providing visibility and control over containerized applications, was deployed and evaluated. However, it was not fully integrated at Adfinis, and no process existed for its implementation into customer environments.

Objectives

This thesis aims to address these challenges through three main objectives: configuring StackRox security policies to meet Adfinis‘s needs, integrating StackRox into existing security processes within Adfinis‘s Information Security Management System (ISMS), and developing deployment scenarios for implementation in both new (greenfield) and existing (brownfield) customer projects.

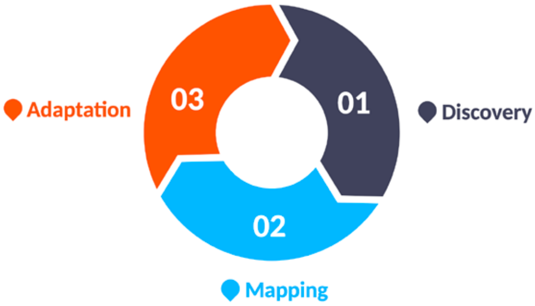
Results

The analysis of StackRox‘s default policies showed they provide effective security and fit well with Adfinis‘s requirements, with minor gaps to be addressed within the ISMS. Integration into Adfinis‘s ISMS provided a structured approach to incorporate StackRox into existing processes, improving vulnerability and risk management. Additionally, a process for integrating StackRox into customer environments was created, with detailed scenarios for both greenfield and brownfield projects.

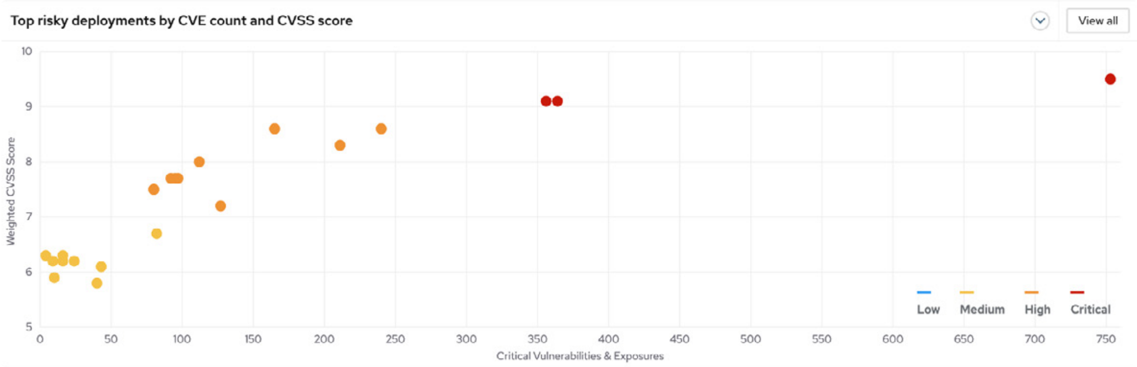
Future Directions

This thesis laid the groundwork for implementing StackRox at Adfinis and in customer environments. The outlined processes need testing in real customer projects to refine and optimize StackRox integration. Continuous improvement involves refining security policies and expanding training programs.

Mario Lars Hadorn
IT Security



Deployment Scenarios Big Picture



StackRox: CVE Graph on a Azure Test Cluster